UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,184	12/15/2003	Yuuki Miyazaki	25880	2153

20529 7590 04/02/2007

NATH & ASSOCIATES
112 South West Street
Alexandria, VA 22314

EXAMINER	
ZEE, EDWARD	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/734,184	MIYAZAKI, YUUKI	
	Examiner	Art Unit	
	Edward Zee	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 December 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/12/04, 12/21/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the original filing of December 15, 2003. Claims 1-6 are pending and have been considered below.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: product number 23, serial number 24 and license code 25 in regards to figure 2. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities: the examiner notes the use of acronyms (ie. RSA, LAN, CD-ROM, etc.) throughout the specification without first including a description in plain text, as required.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprong et al. (6,134,659) in view of Hicks et al. (5,982,892), and in further view of Hillier et al. (6,055,636).

Examiner's Note: The applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claims 4, 5 and 6 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claims 1 and 4: Sprong et al. discloses a license management method and system comprising:

a. attaching an identification code*(identification number)* to the software product [column 9, lines 44-46];

b. sending identification code*(identification number)* and terminal code*(serial number)* to authentication server*(remote authorization unit)* [column 10, lines 19-23];

c. a recording step, by said authentication server*(remote authorization unit)*, of comparing the identification code and the terminal code with the license information recorded in the database and, if a predetermined condition is satisfied, recording*(collecting)* the identification code and the terminal code in the database [column 10, lines 23-30];

d. a digital signature step, by said authentication server, signing the identification code and the terminal code into an authorization code*(authorization code algorithm)* [column 10, lines 30-41];

e. a checking step, by said user terminal, of checking validity of the authorization code received from the authorization server*(remote authorization unit)* [column 10, lines 49-51];

f. and a limitation release step, by said user terminal, of releasing a functional limitation of the software*(enabling the use of the software)* based on the checking result of said checking step [column 10, lines 60-66].

However, Sprong et al. does not explicitly disclose:

a. a first digital signature creation step of creating, by said product management server, a first digital signature from the identification code using a private key of said product management server, said first digital signature being attached to the software product;

b. a second digital signature creation step, by said route server, of obtaining a public key of said product management server from said product management server and creating a second digital signature from the public key of said product management server using a private key of said route server;

c. a third digital signature creation step, by said route server, of obtaining a public key of said authentication server from said authentication server and creating a third digital signature from the public key of said authentication server using the private key of said route server;

d. a first checking step, by said authentication server, of checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said product management server;

e. a second checking step, by said authentication server, of checking validity of the first digital signature using the public key of said product management server in response to the first digital signature and the terminal code from said user terminal and, based on the checking result, obtaining the identification code;

f. a third checking step, by said user terminal, of checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said authentication server.

g. a fourth checking step, by said user terminal, of checking validity of the fourth digital signature using the public key of said authentication server obtained in said third checking step and, based on the checking result, obtaining the identification code and the terminal code;

Nonetheless, Hicks et al. discloses a similar license management method and system and further discloses:

a. a digital signature creation step of creating, by a product management server*(product key generator)*, a digital signature from the identification code using a private key of said product management server, said digital signature being attached to the software product [column 1, lines 46-51 and column 6, lines 42-47];

b. a checking step, by a user key verifier, of checking validity of the first digital signature using the public key of said product management server*(product key generator)* in response to the first digital signature from said user terminal and, based on the checking result, obtaining the identification code*(product-identifying information)* [column 8, lines 46-56 and column 6, lines 42-47];

c. a fourth digital signature creation step, by said authentication server*(user key generator)*, of creating a fourth digital signature from the identification information using a private key*(random or pseudorandom integer)* of said authentication server [column 7, 7-10]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to digitally sign the identification code and confirm the validity of the signature at the authentication server disclosed by Sprong et al. using the private key of the product management server; and also use public key cryptography when digitally signing the identification code and terminal code of the authentication server. One would have been motivated to do so in order to increase the security and further prevent tampering by using a proven form of cryptography. Though, neither explicitly discloses:

a. a second digital signature creation step, by said route server, of obtaining a public key of said product management server from said product management server and creating a second digital signature from the public key of said product management server using a private key of said route server;

b. a third digital signature creation step, by said route server, of obtaining a public key of said authentication server from said authentication server and creating a third digital signature from the public key of said authentication server using the private key of said route server;

c. a first checking step, by said authentication server, of checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said product management server;

d. a third checking step, by said user terminal, of checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said authentication server.

The examiner notes that it is old and well known in the cryptographic art to further digitally sign a signature public key with a private key of a certificate authority{route server} and to use the trusted public key of the certificate authority{route server} to verify the signature public key. Hillier et al. discloses this in column 1, lines 45 through 65. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to employ a route server to create digital signatures of the authentication server's and product management server's public keys disclosed by Sprong et al. and Hicks et al. and validate these digital signatures by using the public key of the route server. One would have been motivated to do so in order to further prevent tampering or any other malicious activity.

Claims 2 and 5: Sprong et al., Hicks et al. and Hillier et al. disclose a license management method and system as in claims 1 and 4 above and Hillier et al. further discloses that the digital certificates have expiration dates [column 2, lines 4-7], but does not explicitly disclose that the authentication server has a server expiration date indicating an expiration date of the third digital signature, wherein, in said third digital signature creation step, said route server obtains the public key of said authentication server and the server expiration date from said authentication server and, using the private key of said route server, creates a digital signature of said

authentication server from the public key of said authentication server and the server expiration date, and wherein, in said third checking step, said user terminal checks validity of the digital signature of said authentication server using the public key of said route server obtained from said route server and obtains the server expiration date and the public key of said authentication server, further comprising a comparison step of comparing the server expiration date with a current date, said server expiration date being verified as valid in said third checking step. However, it would have been obvious to one of ordinary skill in the art at the time of invention to set an expiration date for the digital signature of the authentication server and to verify that the expiration date is valid. One would have been motivated to do so in order to increase the reliability of the signature verification public key certificates and the encryption public key certificates by employing a key and life cycle management process.

Claims 3 and 6: Sprong et al., Hicks et al. and Hillier et al. disclose a license management method and system as in claims 1 and 4 above and Sprong et al. further discloses that the authentication server has a software expiration date indicating an expiration date of the software*(duration and extend of authorized use)*, wherein, in said fourth digital signature creation step, a digital signature of said terminal is created from the identification code, the terminal code, and the software expiration date using the private key of said authentication server, wherein, in said fourth checking step, said user terminal checks validity of the fourth digital signature using the public key of said authentication server obtained from said authentication server and obtains the identification code, the terminal code, and the software expiration date, and wherein, in said limitation release step, the functional limitation of the installed software is released [column 9, lines 46-57], but does not explicitly disclose that the

limitation release step is based on the software expiration date verified as valid in said fourth checking step.

However, it would have been obvious to one of ordinary skill in the art at the time of invention to have the user terminal verify the expiration date of the software to be valid before releasing the functional limitation of the software. One would have been motivated to do so in order to prevent unauthorized users from using their software after the license has expired.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Ahmad (5,925,127), Yuval et al. (5,586,186) and DeMello et al. (7,017,189).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ

EZ
March 18, 2007

James W. Myhre
Supervisory Patent Examiner